REMARKS

Claims 1-30 are pending in this application, with claims 1, 12, 21 and 29 being independent. Reconsideration and allowance of the above-referenced application are respectfully requested.

Claims 1-30 stand rejected under 35 U.S.C. § 102(b) as allegedly being anticipated by Trostle (U.S. Patent No. 5,919,257). This contention is respectfully traversed.

Trostle describes examining executable programs during pre-boot of a workstation to determine if any illicit changes have been made to the selected executable programs; and if changes are detected, the user and/or administrator is notified. (*See* Trostle at col. 1, line 66 to col. 3, line 3.) This is clearly different than "examining a set of instructions embodying an invoked application to identify the invoked application", as recited in independent claim 1.

The executable programs of Trostle are deliberately examined during pre-boot, which is before the applications are invoked. The current rejection unreasonably disregards the word "invoked" in the claims. Based on the Specification, all of claims 1-28 are clearly limited to examining a set of instructions embodying an application that has been activated and is running. (*See e.g.*, Specification at ¶s 19-20 and 29.) This is the exact opposite of Trostle, where the objective is to

detect illicit changes before the workstation boots up. Thus, claims 1-28 should be in condition for allowance for at least this reason.

In addition, independent claim 1 recites, "examining a set of instructions embodying an invoked application to identify the invoked application; obtaining an application-specific intrusion detection signature; and monitoring network communications for the invoked application using the application-specific intrusion detection signature to detect an intrusion." (Emphasis added.) The Specification explicitly defines "intrusion" as "an attempt to break into and/or misuse a computing system", and explicitly defines "intrusion signature" as "a communication pattern identified as corresponding to a known type of intrusion, including patterns that may be found in individual packets and patterns that may be gleaned from analyzing multiple packets." (*See* Specification at ¶ 18.)

The cited portions of Trostle (col. 5, lines 28-42; and col. 6, lines 13-17) describe the use of signed pre-boot modules to enhance security between workstation and server, and a signature "used for background authentication and to further assist in validating the authenticity of packets transmitted by the workstation onto the network." The "signatures" being described here are clearly referring to digital signature

techniques (e.g., encrypting a pre-boot module with a private key of a private-public key pair). (*See* Trostle at col. 5, lines 32-46.) This is completely different than the claimed obtaining an application-specific intrusion detection signature, and monitoring network communications for the invoked application using the application-specific intrusion detection signature to detect an intrusion. As described in the Specification:

> The present inventor recognized the potential advantages of providing network intrusion detection systems and techniques that accurately identify and take into consideration the network applications currently running on a computing system/machine in a networked environment. When applications invoked on a networked machine are accurately identified, network communications for invoked applications may be monitored for application-specific intrusion signatures, and abnormal application behavior may be detected. Moreover, intrusion signatures and behavior criteria may be dynamically loaded from a remote security operation center.

(See Specification at ¶ 19.)

Trostle does not describe monitoring network communications as claimed; Trostle's focus is pre-boot detection of prior illicit changes to executable programs. As the examiner may readily discover and as is well known to the artisans in this

field, Trostle's pre-boot detection is very different from the recited network communications monitoring. In the Final Office Action, the examiner apparently overlooks this difference and states, "Trostle teaches intrusion detection programs are commonly used in order to detect unauthorized modifications of executable programs (col. 1, lines 39-41)." (*See* Final Office Action mailed January 13, 2006 at page 10.) It should be noted that this citation is to the Background section of Trostle, and ignores the rest of the paragraph:

> Intrusion detection programs (i.e., virus checking programs) are commonly used in order to detect unauthorized modifications to executable programs. However, a particular problem with these intrusion detection programs is that they operate only after the operating system has been started. Therefore, the intrusion detection program is untrusted, and can be altered by a hacker since it operates after the operating system has initiated operation. [...] Therefore, the integrity of a[n] intrusion detection program which operates following system boot is suspect due to its vulnerability to attack, by for example, a Trojan horse.

(*See* Trostle at col. 1, lines 39-54.) Thus, the above quoted portion in Trostle actually teaches away from monitoring of network communications for an invoked application. Trostle does not describe in either his "Summary of the Invention" or his

"Description of a Preferred Embodiment" sections monitoring network communications as claimed, and Trostle's brief mentioning of "[i]ntrusion detection programs (i.e., virus checking programs)" in his Background section does not interrelate with the other cited portions of Trostle to someone anticipate the presently claimed subject matter. Thus, it is respectfully suggested that claims 1-30 should be in condition for allowance.

Dependent claims 2-11, 13-20, 22-29, and 30 should be patentable based on the above arguments and the additional recitations they contain. For example, with respect to claims 2, 13, and 30, the cited portion of Trostle (col. 3, lines 19-30) describes how the hash function and the trusted hash value can be downloaded during pre-boot in a manner that is transparent to the user and provides a trusted technique for detecting illicit changes to executable programs. Trostle describes detecting whether an original application has been modified by a rogue piece of software, not tracking network actions taken by the application. Trostle does not describe tracking one or more characteristics of network communications to identify process-specific abnormal communication behavior. The previously presented arguments regarding this clear distinction between Trostle and the present claims have not been

addressed. Since nothing in Trostle can be even remotely considered similar to this claimed subject matter, reconsideration of the rejection of claims 2, 13, and 30 is respectfully requested.

Claim 3 recites, "wherein tracking one or more characteristics of the network communications comprises comparing the one or more characteristics with one or more configurable thresholds." The cited portion of Trostle (col. 5, lines 50-52) describes login authentication for a user. This bears no relation whatsoever to the claimed subject matter. Thus, reconsideration of the rejection of claim 3 is respectfully requested.

Claim 4 recites, "wherein at least one of the one or more configurable thresholds comprises a threshold set by monitoring communications for the invoked application during a defined time window." The cited portion of Trostle (col. 1, line 66 to col. [2], line 3) states, "Briefly, according to the present invention, during pre-boot (i.e., the period of time prior to initiating operation of the workstation operating system), a networked workstation performs an intrusion detection hashing function on selected workstation executable program(s)." This bears no relation whatsoever to the claimed subject matter.

Thus, reconsideration of the rejection of claim 4 is respectfully requested.

Claims 5 and 14 recite, "wherein monitoring network communications comprises monitoring network communications in a network intrusion detection system component invoked with the invoked application." (Emphasis added.) As discussed above, Trostle describes detection operations performed before the operating system is booted, and thus cannot be considered to describe invoking a network intrusion detection system component with the invoked application, as claimed. (*See e.g.*, the Specification at ¶ 38.) Moreover, the cited portion of Trostle (col. 1, lines 39-41) merely states, "Intrusion detection programs (i.e., virus checking programs) are commonly used in order to detect unauthorized modifications to executable programs." This clearly does not anticipate the claimed subject matter since it says nothing about when or how the intrusion detection programs are invoked. Thus, reconsideration of the rejection of claims 5 and 14 is respectfully requested.

Claims 6 and 15 recite, "wherein the network intrusion detection system component and the invoked application run within a single execution context." The Specification explicitly defines "execution context" as "a set of processing cycles given to a process, such as a task in a multitasking

operating system." (*See* Specification at ¶ 17.) The cited portion of Trostle (col. 4, lines 32-35) describes a NIC (Network Interface Card) that includes a BIOS ROM (Basic Input/Output System Random Access Memory) that contains program instructions executed in the CPU (Central Processing Unit) during initialization in order to initiate downloading of executable pre-boot software modules resident on a server. This bears no relation whatsoever to the claimed subject matter. Thus, reconsideration of the rejection of claims 6 and 15 is respectfully requested.

For the rejections of claims 7-11, 16-20, and 22-28, the cited portions of Trostle also bear no relation whatsoever to the claimed subject matter. Thus, reconsideration of the rejection of claims 7-11, 16-20, and 22-28 is respectfully requested.

It is believed that all of the pending claims have been addressed. However, the absence of a reply to a specific issue or comment does not signify agreement with or concession of that issue or comment. Because the arguments made above may not be exhaustive, there may be reasons for patentability of any or all pending claims (or other claims) that have not been expressed. Finally, nothing in this paper should be construed as an intent to concede any issue with regard to any claim, except as

specifically stated in this paper, and the amendment of any claim does not necessarily signify concession of unpatentability of the claim prior to its amendment.

It is respectfully suggested for all of these reasons, that the current rejections are overcome, that none of the cited art teaches or suggests the features which are claimed, and therefore that all of these claims should be in condition for allowance. A formal notice of allowance is thus respectfully requested.

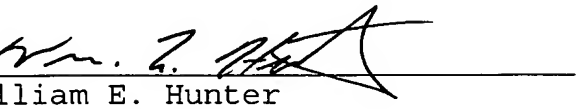
This Response is filed with a Request for Continued Examination (RCE) and an Information Disclosure Statement (IDS). The pending claims should be patentable over the cited references. Consideration of the submitted references and the above arguments is respectfully requested.

The undersigned would like to avoid the necessity of filing an appeal. Thus, in the absence of a forthcoming notice of allowance, a telephone interview with the examiner is respectfully requested to resolve any remaining issues.

A check for $790 is enclosed to cover the RCE filing fee. Please apply any other necessary charges or credits to Deposit Account No. 06-1050.

Respectfully submitted,

Date: April 13, 2006



William E. Hunter
Reg. No. 47,671
Attorney for Intel Corporation

Fish & Richardson P.C.
PTO Customer No. **20985**
12390 El Camino Real
San Diego, California 92130
(858) 678-5070 telephone
(858) 678-5099 facsimile

10590335.doc